Guo, Fuchun; Mu, Yi; Susilo, Willy; Varadharajan, Vijay
Membership encryption and its applications. (English) [Zbl 1316.94076]
Boyd, Colin (ed.) et al., Information security and privacy. 18th Australasian conference, ACISP 2013,

Summary: We propose a new encryption primitive called Membership Encryption. Let \( P(G) \) be a privacy-preserving token on a group attribute/identity \( G \), such that given \( P(G) \) it is hard to know the attributes in \( G \). In this membership encryption, if an encryption takes as input an attribute \( A \) and the token \( P(G) \), the decryption requires holding the membership \( A \in G \), i.e., \( A \) belongs to this group attribute. Membership encryption is applicable in constructing membership proof \( A \in P(G) \) with privacy preserving on group attribute and the membership. Membership encryption can be also utilized to construct an efficient two-round \( K \)-out-of-\( N \) oblivious transfer protocol. In this paper, we construct a provably secure membership encryption where the group token \( P(G) \) is constant-size with maximum number accountability on attributes. Using our scheme, the proposed oblivious transfer protocol exhibits the nice feature of \( O(1) \) communication cost for any \( K \) from receiver to sender, and \( O(N) \) communication cost from sender to receiver.

For the entire collection see [Zbl 1264.94003].

MSC:
94A60 Cryptography

Cited in 4 Documents

Full Text: DOI